Amendments to the Claims:

This listing of claims will replace all prior versions, and listings of claims in the application:

Listing of Claims:

1. (Currently amended): An electronic authentication method comprising:

generating an identifier ~~for~~ that is associated with contents in a first information processing apparatus;

~~storing said identifier in a storage unit;~~

combining said contents and said identifier to produce enhanced content;

transmitting said ~~contents and said identifier~~enhanced content to a second information processing apparatus;

presenting said enhanced content to a user at said second information processing apparatus, said identifier being combined with said contents in a manner that it is visually imperceptible to said user;

~~inputting~~ receiving user data ~~for said contents~~ in said second information processing apparatus~~;~~ and in response thereto producing input data from said user data, including obtaining said identifier from said enhanced contents, wherein said input data is produced based on said identifier; and

transmitting said input data ~~and said identifier~~ from said second information apparatus to said first information apparatus as received input data~~; and~~

~~authenticating legitimacy of said input data and invalidating said stored identifier if said received identifier matches said identifier in said storage unit in said first information processing apparatus~~.

2. (Currently amended): An electronic authentication method according to claim 1, further comprising:

generating a second identifier at said first information processing apparatus;

storing said second identifier in a storage unit as a stored identifier;

incorporating said second identifier into said input data; and

in said first information processing apparatus, authenticating legitimacy of said input data and invalidating said stored identifier if said second identifier in said input data matches said stored identifier~~wherein in said first information processing apparatus, said identifier is embedded in said contents prior to transmission of said contents to said second information processing apparatus~~.

3. (Currently amended): An electronic authentication method according to claim ~~2~~1, wherein said identifier is an encryption key, wherein~~said method further comprising:~~

said step of combining includes embedding ~~an~~ said encryption key in said contents in said first information processing apparatus prior to transmission of said contents to said second information processing apparatus;

said step of producing includes encrypting said ~~input~~ user data in said second processing apparatus by using said encryption key prior to transmission of said input data to said first information processing apparatus; and

said method further comprising decrypting said received input data in said first information processing apparatus.

4. (Currently amended): An electronic authentication method according to claim 3, wherein: said embedded encryption key is a public key; said received input data is decrypted using a private key associated with said public key; and said public key and said private key are generated in said first information processing apparatus.

5. (Currently amended): An information processing method comprising:

generating an identifier for contents;

storing said identifier as a stored identifier;

generating a second identifier;

incorporating said identifier and said second identifier with said contents to produce enhanced contents such that when said enhanced contents is displayed to a user, said identifier and said second identifier are visually imperceptible;

transmitting said enhanced contents ~~and said identifier~~ to an external apparatus;

receiving received data from said external apparatus;

acquiring an acquired identifier for said contents; and

carrying out processing based on said received data and invalidating said stored identifier if said acquired identifier matches said stored identifier.

6. (Canceled)

7. (Currently amended): An information processing method according to claim ~~6~~5, wherein said second identifier is an encryption key, said method further comprising:

~~embedding an encryption key in said contents prior to transmission of said contents to said external apparatus; and~~

receiving an identifier encrypted by using said encryption key and decrypting said received encrypted identifier.

8. (Currently amended): An electronic authentication system comprising a first information processing apparatus and a second information processing apparatus wherein:

said first information processing apparatus comprises:

a means for generating an identifier for contents;

a storage means for storing at least a first portion of said identifier as a stored identifier; and

a means for transmitting ~~said~~ enhanced contents and said identifier to said second information processing apparatus, including embedding means for embedding said identifier in said contents to produce said enhanced contents;

said second information processing apparatus comprises:

a means for inputting user data ~~for said received contents~~, including means for displaying received enhanced contents such that said identifier is not visually perceivable by a user; and

a means for transmitting said ~~input~~ user data and said identifier to said first information processing apparatus as input data, wherein said input data is generated by

processing said user data and said first portion of said identifier based on a second portion of said identifier; and

there is further provided a processing means for authenticating legitimacy of said input data received by said first information processing apparatus and invalidating said stored identifier if said first portion of said identifier contained in said input data~~received by said first information processing apparatus~~ matches said stored identifier~~stored in said storage means~~.

9. (Currently amended): An electronic authentication system according to claim 8, wherein said second information processing apparatus further comprises an acquirement means for acquiring said identifier from said received enhanced contents~~first information processing apparatus further includes an embedding means for embedding said identifier in said contents; and said first information processing apparatus transmits said contents including said embedded identifier to said second information processing apparatus~~.

10. (Currently amended): An electronic authentication system according to claim ~~9~~8, wherein ~~said first information processing apparatus transmits said contents, said contents further including~~ said second portion of said identifier is an ~~embedded~~ encryption key~~, to said second information processing apparatus~~; and said first information processing apparatus further comprises a reception means for receiving an identifier encrypted by using said encryption key and decrypting said encrypted identifier.

11. (Currently amended): An information processing apparatus comprising:

a generation means for generating an identifier for contents, said identifier comprising a first part and a second part;

a storage means for storing at least said first part of said identifier as a stored identifier;

a transmission means for transmitting said contents and said identifier to an external apparatus as enhanced contents, wherein said enhanced contents comprises said identifier embedded in said contents such that upon displaying said enhanced contents to a user, said identifier is substantially visually imperceptible;

a reception means for receiving received data from said external apparatus;

an acquirement means for acquiring an acquired identifier ~~for said contents~~ from said received data; and

a processing means for carrying out processing based on said received data and invalidating said stored identifier ~~stored in said storage means~~ if said acquired identifier matches said stored identifier.

12. (Canceled)

13. (Currently amended): An information processing apparatus according to claim ~~12~~11, wherein ~~said transmission means transmits said contents further including said embedded~~ second portion of said identifier is an encryption key ~~to said external apparatus~~; and there is further provided a reception means for receiving an identifier encrypted by using said encryption key and decrypting said received encrypted identifier.

14. (Currently amended): An information processing apparatus comprising:

a contents requesting means for requesting an external information processing apparatus to transmit contents;

a reception means for receiving said requested contents ~~and~~, an identifier being embedded in said requested contents;

a display means for displaying said requested contents to a user, wherein said identifier is substantially visually imperceptible;

an extraction means for extracting said identifier from said requested contents;

an input means for inputting user data ~~for said contents~~from a user; and

a transmission means for transmitting, as secured data, said ~~input~~ user data and a first portion of said identifier to said external information processing apparatus, said secured data being generated using a second portion of said identifier.

15. (Currently amended): An information processing apparatus according to claim 14, wherein said second portion of said identifier is an encryption key, said apparatus

further comprising an encryption means for encrypting said ~~input~~ user data by using ~~an~~ said encryption key ~~additionally embedded in said contents received by said reception means~~.

16. (Currently amended): A storage medium for storing information readable by a computer, said medium characterized in that said information includes:

a generation function for generating an identifier for contents;

a storage function for storing a first portion of said generated identifier;

a transmission function for transmitting said contents and said identifier to an external apparatus as enhanced content, wherein said generated identifier is embedded in said contents such that upon displaying said enhanced contents to a user, said generated identifier is substantially visually imperceptible;

a reception function for receiving data from said external apparatus;

an acquirement function for acquiring an identifier for said contents from said received data; and

a processing function for authenticating legitimacy of said received data and invalidating said stored identifier if said acquired identifier matches said stored identifier.

17. (Canceled)

18. (Currently amended): A storage medium for storing information readable by a computer according to claim ~~17~~16, ~~said medium characterized in that: said transmission function transmits said contents further including said embedded~~ wherein said generated identifier includes a second portion that is an encryption key ~~to said external apparatus~~; and said information further includes a function for receiving said data encrypted by using said encryption key and decrypting said received encrypted data.

19. (Currently amended): A storage medium for storing information readable by a computer, said medium characterized in that said information includes:

a contents requesting function for requesting an external information processing apparatus to transmit contents;

a reception function for receiving said requested contents, ~~and~~ an identifier embedded in said contents;

a display function for displaying said requested contents to a user, wherein said identifier is substantially visually imperceptible;

an extraction function for extracting said identifier from said contents;

an input function for inputting user data from a user~~for said contents~~; and

a transmission function for transmitting, as ~~said~~ input data, said user data and a first portion of said identifier to said external information processing apparatus, said input data being generated using a second portion of said identifier.

20. (Currently amended): A storage medium for storing information readable by a computer according to claim 19, wherein said second portion of said identifier is an encryption key, said medium characterized in that said information further includes a function for encrypting said ~~input~~ user data by using ~~an~~ said encryption key ~~additionally embedded in said contents received by said reception function~~.

21. (Currently amended): An electronic authentication method comprising:

generating an identifier for contents in a first information processing apparatus;

driving said first information processing apparatus to store a first portion of said identifier and the present time as a storage time in a storage unit;

transmitting said contents and said identifier to a second information processing apparatus as enhanced content, wherein said identifier is embedded in said contents;

presenting said enhanced content to a user at said second information processing apparatus, said identifier being visually imperceptible to said user;

inputting user data ~~for said contents~~from a user received by said second information processing apparatus in said second information processing apparatus;

transmitting, as secured data, said ~~input~~ user data and said first portion of said identifier from said second information processing apparatus to said first information processing apparatus, said secured data being generated based on a second portion of said identifier; and

invalidating said first portion of said identifier stored in said storage unit if said identifier received by said first information processing apparatus is not stored in said storage unit or a time of a predetermined length has lapsed since said storage time stored in said storage unit.

22. (Currently amended): An electronic authentication method, comprising:

generating an ~~identifier for an access to~~encryption key that is associated with contents in a first information processing apparatus;

~~storing said identifier in a storage unit;~~embedding said encryption key into said contents to produce enhanced content such that when said enhanced content is displayed to a user said encryption key is substantially imperceptible;

transmitting said ~~contents and said identifier~~enhanced content to a second information processing apparatus;

displaying said enhanced content in said second information processing apparatus;

inputting user data ~~for said contents~~from a user that has been received by said second information processing apparatus in said second information processing apparatus;

encrypting said user data using said encryption key to produce secured input data, including acquiring said encryption key from said enhanced content;

transmitting said secured input data ~~and said identifier~~ from said second information processing apparatus to said first information processing apparatus; and

validating said secured input data by decrypting said secured input data with a decryption key~~only for this transaction if said identifier received by said first information processing apparatus matches said identifier stored in said storage unit~~.

23. (Canceled)

24. (Currently amended): An authentication method in a system in which a first computer making a request for a service is connected to a second computer rendering services via a network, requested contents being transmitted from the second computer to the

first computer, data being transmitted from the first computer to the second computer associated with the contents, said method comprising:

generating at the second computer an access number for accessing the contents and cataloging the access number in a storage unit;

embedding the access number in the contents to produce enhanced content so that the access number is ~~invisible~~ substantially visually imperceptible when the enhanced content is displayed and transmitting the ~~contents~~ enhanced content to the first computer;

displaying the contents at the first computer;

generating secured data at the first computer by processing user-provided data with ~~adding~~ the access number fetched from the ~~contents~~ enhanced content ~~to data inputted associated with the contents~~ and transmitting the ~~inputted~~ secured data to the second computer; and

authenticating validity ~~at the second computer~~ of the ~~received~~ secured data by decrypting the secured data received at the second computer with a decryption key ~~when the received access number has been cataloged and invalidating the cataloged access number~~.

25. (Currently amended): An authentication method according to claim 24, wherein the ~~second computer generates~~encryption key is a public key and the decryption key is a private key ~~for accessing the contents and catalogs the public key and the private key in the storage unit, embeds the public key in the contents so that the public key is invisible and transmits the contents to the first computer, allows the first computer to encrypt data on inputted associated with the contents by the public key fetched from the contents and transmit the data to the second computer, and decrypt the received data by the public key cataloged when the received access number has been cataloged~~.

26 - 28. (Canceled)

29. (Currently amended): A server apparatus comprising:

a processor;

a storage device;

a network interface; and a bus interconnecting said processor, said storage device and said network interface;

wherein said processor generates an ~~identifier~~ encryption key for contents ~~and stores said identifier into said storage device~~; and wherein said processor transmits enhanced content comprising said contents and said ~~identifier~~ encryption key to an external apparatus via said network interface such that when said enhanced content is displayed said encryption key is substantially visually imperceptible; and wherein said processor receives data from said external apparatus via said network interface, said data being encrypted with said encryption key; ~~and thereupon acquires from said data an identifier for said contents from said received data; and wherein said processor performs processing based on said received data and invalidates said identifier stored in said storage means if said acquired identifier matches said stored identifier~~.

30. (Currently amended): A server apparatus according to claim 29, wherein in said encryption key is a public key component of a public key and private key encryption method~~apparatus, said processor further embeds said identifier in said contents; and wherein said processor transmits said contents including said embedded identifier to said external apparatus~~.

31. (Canceled)

32. (Currently amended): A client apparatus comprising:

a processor;

an input device;

a network interface; and a bus interconnecting said processor, said input device and said network interface;

wherein said processor requests an external information processing apparatus to transmit contents via said network interface; and wherein said processor receives said ~~requested~~ contents and an ~~identifier~~ encryption key embedded in said contents, such that when said content is displayed to a user, said encryption key is substantially visually unperceivable; and thereupon, said processor extracts said ~~identifier~~ encryption key from said contents; and wherein said processor receives ~~input~~ user data ~~for said contents~~ from said input device; and wherein said

processor transmits said ~~input~~ user data ~~and said identifier~~ to said external information processing apparatus via said network interface by encrypting said user data with said encryption key.

a1

33 - 34. (Canceled)